Центр Квантовых Технологий

СФБ ЛАБ

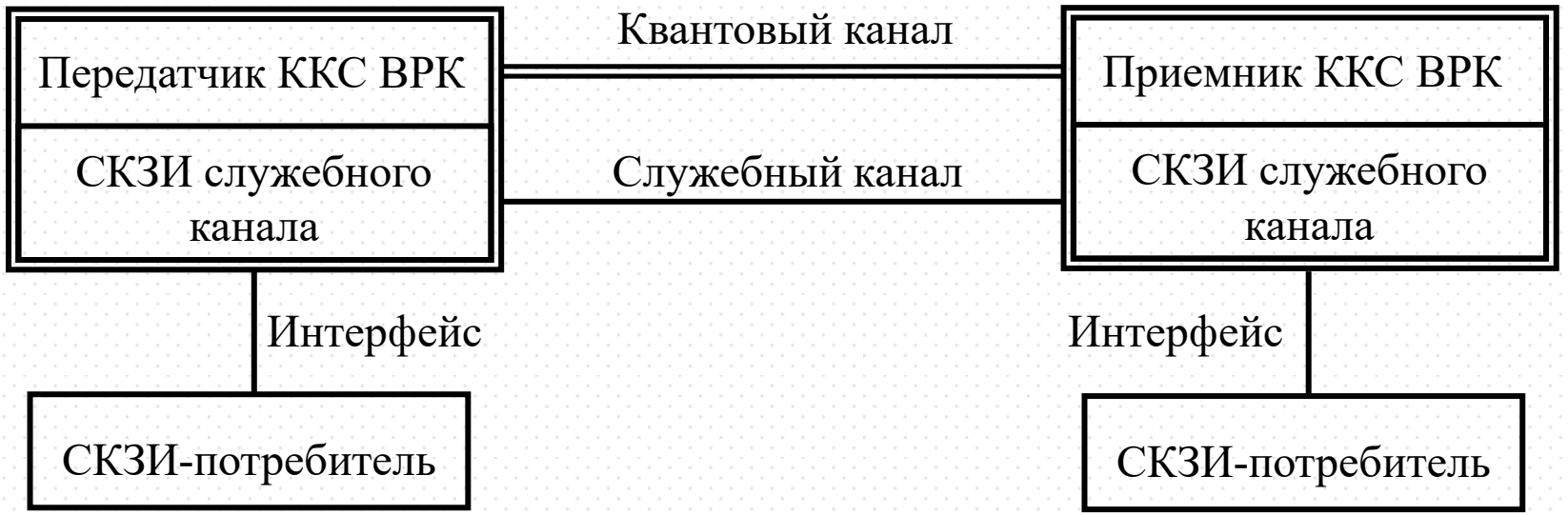
О некоторых принципах квантового распределения ключей с использованием доверенных промежуточных узлов (технологии ДПУ)

Науменко Антон Павлович

Заместитель начальника отдела специальных исследований
и разработок ООО «СФБ Лаб»

Руководитель направления
АО «ИнфоТеКС»

Типовой вариант построения системы квантового распределения ключей



Основные результаты

СФБ ЛАБ

Центр Квантовых Технологий

- Для квантового маршрута из **N** доверенных промежуточных узлов (ДПУ) показана ε-секретность распределяемого квантового ключа в случае доказанной **ε/N**-секретности для каждой пары ДПУ на маршруте (для XOR в качестве алгоритма «перешифрования» на ДПУ)

- Аналогичный по порядку результат может быть получен для случая использования «хороших» алгоритмов блочного шифрования («Кузнечик») в качестве алгоритма «перешифрования» при условии «двойного» (с запасом) шифрования

- Показана принципиальная возможность построения «сети ДПУ» из **N=500** узлов, которая требует ввода только **одного(!)** классического ключа аутентификации служебного канала на каждом ДПУ за предполагаемое время эксплуатации ДПУ (например, **10 лет**)

СФБ ЛАБ

Центр Квантовых Технологий

СПАСИБО ЗА ВНИМАНИЕ!

Anton.Naumenko@infotecs.ru